Linux操作系统下用户和用户配置文件解析Linux认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/555/2021_2022_Linux_E6_93_8D_E4_BD_c103_555851.htm 除了像Windows系统一样新建用户帐户外，在Linux系统中同样有一些用户帐户是在系统安装后就有的，就像Windows系统中的内置帐户一样。如果您想了解Linux系统的一些帐号，可以通过查看/etc/passwd文件实现，如下所示。 root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt mail:x:8:12:mail:/var/spool/mail:/sbin/nologin news:x:9:13:news:/etc/news: uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin operator:x:11:0:operator:/root:/sbin/nologin games:x:12:100:games:/usr/games:/sbin/nologin gopher:x:13:30:gopher:/var/gopher:/sbin/nologin ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/:/sbin/nologin dbus:x:81:81:System message bus:/:/sbin/nologin vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin rpm:x:37:37::/var/lib/rpm:/sbin/nologin haldaemon:x:68:68:HAL daemon:/:/sbin/nologin netdump:x:34:34:Network Crash Dump

user:/var/crash:/bin/bash nscd:x:28:28:NSCD
Daemon:/:/sbin/nologin sshd:x:74:74:Privilege-separated
SSH:/var/empty/sshd:/sbin/nologin rpc:x:32:32:Portmapper RPC
user:/:/sbin/nologin rpcuser:x:29:29:RPC Service
User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS
User:/var/lib/nfs:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
pcap:x:77:77::/var/arpwatch:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
squid:x:23:23::/var/spool/squid:/sbin/nologin
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
gdm:x:42:42::/var/gdm:/sbin/nologin htt:x:100:101:IIIMF
Htt:/usr/lib/im:/sbin/nologin
winda:x:500:500:wangda:/home/winda:/bin/bash
cyrus:x:76:12:Cyrus IMAP Server:/var/lib/imap:/bin/bash
named:x:25:25:Named:/var/named:/sbin/nologin
pegasus:x:66:65:tog-pegasus OpenPegasus WBEM/CIM
services:/var/lib/Pegasus:/sbin/nologin
alice:x:501:501:Alicechen:/home/alice:/bin/bash
exim:x:93:93::/var/spool/exim:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
mailman:x:41:41:GNU Mailing List

Manager:/usr/lib/mailman:/sbin/nologin amanda:x:33:6:Amanda user:/var/lib/amanda:/bin/bash 与用户相关的配置文件主要有两个： /etc/passwd ：用户配置文件； /etc/shadow ：用户影子口令文件； Password文件内容参见上面内容，只有root帐户才有权限修改。该文件中包含了系统中所有用户的用户名和它们的相关信息。每个用户帐号在文件中对应一行，并且用冒号（；）分为7个部分（Linux系统中称为“域”），各部分间用冒号（:）分隔。格式如下： 帐户名:是否有加密口令:用户ID:组ID:帐户全名或描述:登录目录:登录shell 如上面列出的root用户在此文件中所对应的行为： root:x:0:0:root:/root:/bin/bash 它表示root帐户的是有密码的（以x表示，没有x的表示没有设置密码），用户ID和组ID号均为“0”（内置帐户的用户ID和组ID均小于500，而新建的帐户用户ID和组ID均等于或大于500），帐户全名为root，所用的登录shell有为/bin/bash。 /etc/passwd文件对系统的所有用户都是可读的，这样的好处是每个用户都可以知道系统上有哪些用户，但缺点是其他用户的口令容易受到攻击（尤其当口令较简单时）。所以在像红帽子和红旗等品牌Linux中均使用影子口令格式，将用户的口令存储在另一个文件/etc/shadow中，该文件只有根用户root可读，因而大大提高了安全性。如下所示： root:1qnvzih07$LKCr9gldeq1ajos5tuLPH.:13670:0:99999:7::: bin:*:13670:0:99999:7::: daemon:*:13670:0:99999:7::: adm:*:13670:0:99999:7::: lp:*:13670:0:99999:7::: sync:*:13670:0:99999:7::: shutdown:*:13670:0:99999:7::: halt:*:13670:0:99999:7::: mail:*:13670:0:99999:7:::

news:*:13670:0:99999:7::: uucp:*:13670:0:99999:7:::
operator:*:13670:0:99999:7::: games:*:13670:0:99999:7:::
gopher:*:13670:0:99999:7::: ftp:*:13670:0:99999:7:::
nobody:*:13670:0:99999:7::: dbus:!!:13670:0:99999:7:::
vcsa:!!:13670:0:99999:7::: rpm:!!:13670:0:99999:7:::
haldaemon:!!:13670:0:99999:7::: netdump:!!:13670:0:99999:7:::
nscd:!!:13670:0:99999:7::: sshd:!!:13670:0:99999:7:::
rpc:!!:13670:0:99999:7::: rpcuser:!!:13670:0:99999:7:::
nfsnobody:!!:13670:0:99999:7::: mailnull:!!:13670:0:99999:7:::
smmsp:!!:13670:0:99999:7::: pcap:!!:13670:0:99999:7:::
apache:!!:13670:0:99999:7::: squid:!!:13670:0:99999:7:::
webalizer:!!:13670:0:99999:7::: xfs:!!:13670:0:99999:7:::
ntp:!!:13670:0:99999:7::: gdm:!!:13670:0:99999:7:::
htt:!!:13670:0:99999:7:::
winda:1EzhNNTg6$Zgh0TrLsnuAnWOdb2w1ut.:13670:0:99999:7::: cyrus:!!:13670:::::: named:!!:13670:::::: pegasus:!!:13670::::::
alice:1vw2uWRMJ$l20TPyj1M3L8x2uqUN/wn.:13670:0:99999:7::: exim:!!:13670:::::: postfix:!!:13670:::::: mailman:!!:13670::::::
amanda:!!:13670:::::: 同样，在这个文件中，也是每个用户对应一行，并且用冒号分成九个部分（Linux系统中称为“ 域 ”）。每一行的格式如下： 用户登录名 用户加密后的口令（若为空，表示该用户不需口令即可登录，若为*号，表示该帐号被禁用） 从1970年1月1日至口令最近一次被修改的天数 口令在多少天内不能被用户修改 口令在多少天后必须被修改（0为没有修改过） 口令过期多少天后用户帐号被禁止 口令在到期多少天内给用户发出警告 口令自1970年1月1日被禁止的天数

保留域 同样以root帐户为例，它在上面的代码为：root:1qnvzih07$LKCr9gldeq1ajos5tuLPH.:13670:0:99999:7::: 对照上面的格式可以得出，它的用户登录名为root，加密口令为“ 1qnvzih07$LKCr9gldeq1ajos5tuLPH. ”（因为是加密的，所以显示的并不是直接的口令），从1970年1月1日至口令最近一次被修改的天数为13670天，口令不允许修改，口令在99999天后必须被修改，口令过期7天后用户帐号被禁止，后面的3个域没有配置。